DEPARTMENT OF THE ARMY
HEADQUARTERS, US ARMY ARMOR CENTER AND FORT KNOX
75 6TH AVENUE
FORT KNOX, KENTUCKY 40121-5717

REPLY TO
ATTENTION OF:

Expires 20 April 2009

IMSE-KNX-IMA 20 April 2007

MEMORANDUM FOR

Commanders, All Units Reporting Directly to This Headquarters
Commanders, Fort Knox Partners In Excellence
Directors and Chiefs, Staff Offices/Departments, This Headquarters

SUBJECT: Fort Knox Policy Memo No. 9-07 – Mobile Computing Devices (MCDs)/Portable Electronic Devices (PEDs) Security

1. References.

a. AR 25-2, Information Assurance, 14 November 2003.

b. AR 25-1, Army Knowledge Management and Information Technology, 15 July 2005.

c. Memo, HQ USAARMC, IMSE-KNX-IM, 27 October 2005, subject: USAARMC Policy Memo No. 10-05 – Computer Administrative Rights.

d. Army Best Business Practice 06-EC-O-0007, "Road Warrior" Laptop Security, Version 1.0, 17 February 2006.

e. Army Best Business Practice 03-EC-M-0003, Wireless Security Standards, Version 1.26, 22 June 2004, updated 1 August 2006.

f. Memo, NETC-EST-IA, 1 August 2006, subject: Updated Guidance on the Management of BlackBerry Devices with Internal Bluetooth Capability.

g. Army Best Business Practice 06-EC-O-0008, Data-At-Rest (DAR) Protection, Version 1.0, 12 October 2006.

h. Memo, HQ USAARMC, IMSE-KNX-IMO, 23 February 2007, subject: Fort Knox Policy Memo No. 2-07 – Data-at-Rest Protection for Mobile Computing Devices (MCDs)

2. Purpose. To establish a policy on the use of PEDs and MCDs.

3. Scope. This memorandum addresses methods and practices to manage risks associated with unclassified MCDs and PEDs. The MCDs are defined as laptops, portable notebooks, tablet PCs, external media, and similar systems. Portable electronic devices are defined as personal digital assistants, hand-held computers, mobile/cellular telephones, BlackBerry devices, two-way

pagers, mobile/cellular telephones with digital imagery/recording devices (still and/or video), wireless e-mail devices, and other devices of similar capability or design.

4. Applicability. This policy applies to all Soldiers, civilians, and contractors who utilize government-owned MCDs/PEDs that connect or are associated with the Fort Knox Campus Area Network (FKCAN).

5. Policy. The following are minimum requirements for all MCDs/PEDs and users that connect or are associated with the FKCAN:

a. All MCDs/PEDs that process and/or store data must be approved, certified, and accredited by the FKCAN Designated Approving Authority.

b. All MCDs/PEDs with radio frequency/wireless, infrared, Bluetooth, and audio/video record capable wireless devices will not be allowed in an area where classified information is discussed or processed and will not be connected to any classified networks. These devices will not be used for storing, processing, or transmitting classified information.

c. Privately-owned MCDs/PEDs will not be used to send, receive, store, process, or transmit DOD information or connect to the FKCAN.

d. Government-owned PEDs will not be connected at any time to privately-owned computer equipment.

e. All MCDs/PEDs will have DOD-approved anti-virus software installed. To ensure consistent levels of protection against viruses, PEDs will maintain up-to-date signature files used to profile and identify viruses, worms, and malicious codes. Anti-virus software and updates for PEDs are available from the DOD Cert website (http://www.cert.mil).

f. All MCDs/PEDs will have identification and authentication (login and password or PIN) measures, and passwords will be in accordance with AR 25-2. If a device has the capability, the password protection feature will not permit its bypass without zeroing all data stored on the device. The password protection features will be enabled at all times.

g. All MCDs/PEDs will have a US Government SF 700 (series) classification label appropriate for the classification level affixed in clear view.

h. All MCDs/PEDs that store data will have the FK Label 5078, Data-At-Rest laptop label affixed to it.

i. Users will maintain serial and model identification numbers, system and domain names, and emergency point of contact information for the MCDs/PEDs separate from the MCDs/PEDs while away from their duty station.

j. Users will secure the MCDs/PEDs at all times when not in use and in their possession. For example, when using a rental car, ensure the MCD/PED is out of sight in a locked vehicle/trunk; be aware of the damage extreme temperatures can do to equipment. Never leave an MCD/PED unattended in public, meetings, conventions, or conferences. Never place MCDs/PEDs in checked or unattended baggage. Use a non-descript carrying case, and close zippers of the case so no one can reach into the bag and remove the MCD/PED. Never leave an unsecured MCD/PED in an unattended hotel room.

k. Users will NEVER download and install software and/or enable unauthorized protocols or services on MCDs/PEDs.

l. Users should avoid using MCDs/PEDs in areas where "shoulder surfing" is easy.

m. Users shall ensure a backup of any MCD/PED data before departure and secure the backup at their normal duty station. The unit/activity Information Assurance Security Officer (IASO)/Information Management Officer (IMO) can assist users with backups.

n. MCDs/PEDs will comply with the Army Best Business Practice for Data-At-Rest requirements. Users of MCDs/PEDs must know what information should be encrypted based on the Army Best Business Practice Data-At-Rest.

o. The Fort Knox Virtual Private Network is the only approved encryption method for data transmission by MCDs across wireless networks to/from wireless devices.

p. For MCDs such as laptops, a firewall and anti-virus software must be used and updated when not connected to the FKCAN.

q. Any MCDs/PEDs that have been away from the duty station must be taken to the IASO and checked for compliancy and contamination prior to connecting to the FKCAN.

r. Users will not use Bluetooth technology/devices with government equipment. The only exception is the BlackBerry CAC Sled. Wireless peripheral devices such as keyboard, printers, etc., are not authorized.

s. Users shall immediately report loss of an MCD/PED to their IASO/IMO, unit commander/director, and intelligence and law enforcement representatives. The IASO/IMO will report the loss to the installation Information Assurance Manager.

t. Per reference c above, users will not be given administrative privileges to MCDs/PEDs because they travel frequently.

u. Users will not connect to more than one active interface at a time (i.e., do not connect to a wireless network and government-wired connection at the same time or to a modem and government-wired connection at the same time). To ensure only one active connection at a time, it is strongly recommended that multiple hardware profiles be set up by the IASO/IMO on each MCD/PED.

FOR THE COMMANDER:

Mark D. Needham
MARK D. NEEDHAM
COL, AR
Garrison Commander

DISTRIBUTION:
A